In re Patent Application of:
KASSER
Serial No. 10/799,371
Filed: **March 12, 2004**

REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application. The independent claims have been amended to more clearly define the present invention over the cited prior art references. The dependent claims have also been amended for consistency. The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in amended independent Claim 1, for example, is directed to a method for securing circulation of an encrypted digital document to be reproduced with a document reader. The method comprises providing a user with a storage device storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated with the storage device.

The method further comprises transmitting to a server over a digital data transmission network from the storage device to the server upon connection of the storage device to the server by a terminal connected to the digital data transmission network and to the storage device information identifying the digital document to be reproduced, and the information list and the identification information of the storage device.

The method further comprises identifying from the server the storage device on the basis of the information

identification of the storage device transmitted to the server. Possible fraudulent use of the storage device is determined based upon the information list that is transmitted to the server. The server compares the identification information in the information list with an authorized or fraudulent document reader list for determining fraudulent use of the storage device. If the storage device is not being fraudulently used, then the method comprises transmitting over the digital data transmission network from the server to the computer terminal a decryption key specific to the digital document to be reproduced, with the decryption key being stored in the storage device. The digital document is decrypted using the stored decryption key by the document reader connected to the storage device. The digital document decrypted by the document reader is reproduced.

Independent Claim 9 is also directed to a method for securing circulation of an encrypted digital document to be reproduced with a document reader, and has been amended similar to independent Claim 1.

Independent Claim 17 is directed to a system for securing circulation of an encrypted digital document to be reproduced with a document reader, and has been amended similar to independent Claim 1.

Independent Claim 25 is also directed to a system for securing circulation of an encrypted digital document to be reproduced with a document reader, and has been amended similar to independent Claim 1.

In re Patent Application of:
KASSER
Serial No. 10/799,371
Filed: March 12, 2004
_____/

II. The Claims Are Patentable Over Chatani Et Al.

The Examiner rejected independent Claims 1, 9, 17 and 25 over the Chatani et al. published patent application. The Chatani et al. application is directed to a product distribution and payment system for limited use or otherwise restricted digital software products. FIG. 1 in Chatani et al. illustrates a block diagram of a computer network system that implements the product distribution and payment system. The Examiner has taken the position that Chatani et al. discloses the claimed invention.

The Applicants submit that the amended claims more clearly define the present invention over the Chatani et al. published patent application. In this respect, the storage device (or smart card) provided to the user stores identification information identifying the storage device and a list identifying the most recent document readers used with the storage device. When the storage device is connected to a server in order to obtain a decryption key, the identification information and the list are transmitted to the server which determines a possible fraudulent use of the storage device by determining whether the document readers in the list are unauthorized or not.

A document reader identified in the list can be determined as unauthorized by comparing the item in the list with a list of authorized as well as unauthorized readers. The Applicant submits that the Examiner has mischaracterized the Chatani et al. application. Reference is directed to paragraph 24 of Chatani et al., which provides:

"For the embodiment illustrated in FIG. 1,

In re Patent Application of:
KASSER
Serial No. 10/799,371
Filed: **March 12, 2004**
_____/

> the network game console **114** also has an interface port for the installation of a memory card **124**. Such a memory card might be implemented as a proprietary card format, or a standard format device, such as PC/MCIA format or a similar card format. The memory card **124** stores various firmware parameters and operating environment data that are specific to the particular network game console **114** that the card is installed in. For example, the memory card can be used to store the identification number (ID) assigned to the particular game console. In certain applications, the memory card can also be used to store certain software products, such as computer games or other programs or content to be played back or executed on the game console." (Emphasis added).

As noted above, Chatani et al. discloses that a memory card stores only one identification number of a game console, but not a list of several identification numbers as in the claimed invention.

In paragraphs 60 and 63 of Chatani et al., Chatani et al. fails to teach or suggest determination of fraudulent or unauthorized readers in the list transmitted. Chatani et al. further fails to suggest determination of a fraudulent use of the storage device when the list transmitted contains an identifier of an unauthorized reader.

Chatani et al. merely teaches the use of a database recording, for each disk purchased, the serial number of a single playback machine and the serial number of the purchased disk and the generation of the decryption key on the basis of these serial

numbers. This is done in order to control the use of different playback machines for reading a same purchased disk. Chatani et al. fails to disclose a playback machine in which a memory card is determined as fraudulent or unauthorized for further use with any disk to be ready the playback machine.

Accordingly, it is submitted that amended independent Claim 1 is patentable over Chatani et al. Amended independent Claims 9, 17 and 25 are similar to amended independent Claim 1. Therefore, it is submitted that these claims are also patentable over Chatani et al. In view of the patentability of amended independent Claims 1, 9, 17 and 25, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the claim amendments and the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182

In re Patent Application of:
KASSER
Serial No. 10/799,371
Filed: **March 12, 2004**

Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents on this 26 day of September, 2007.